POINT MULTIPLICATION ON SUPERSINGULAR ELLIPTIC CURVES DEFINED OVER FIELDS OF CHARACTERISTIC 2 AND 3

Kwang Ho Kim
Department of Algebra, Institute of Mathematics, The State Academy of Sciences
Pyongyang city, Democratic People's Republic of Korea

Christophe Negre
Team DALI/ELIAUS, University of Perpignan, Perpignan, France

Keywords: Supersingular, Eliptic Curve, Coordinate Systems, Mixed Addition, Doubling, Tripling.

Abstract: Elliptic curve cryptosystem protocols use two main operations, the scalar multiplication and the pairing computation. Both of them are done through a chain of basic operation on the curve. In this paper we present new formulas for supersingular elliptic curve in characteristic 2 and 3. We improve best known formulas by at least one multiplication in the field.

1 INTRODUCTION

For elliptic curve cryptosystems, scalar multiplication on the curve is the most important but time-consuming operation. So the research on speeding up this operation continues to get increasing attraction since the elliptic curve cryptography has been proposed (Koblitz 1987, Miller 1986).

The scalar multiplication is generally performed by a chain of elementary curve operations like point addition, point doubling and point tripling. This is the case for example in double and add method (Hankerson et al., 2004) or triple and add method (Page and Smart, 2002). Each curve operation requires several field operations on the point coordinates (addition/subtraction, multiplication and eventually inversion or powering).

Consequently to get an efficient scalar multiplication and an efficient pairing it is important to decrease the number of field operations involved in basic curve operations.

Here we focus on supersingular elliptic curve in characteristic two and three. Projective versions of arithmetic on supersingular elliptic curves have been proposed in characteristic 3 by N. Koblitz (Koblitz, 1998), P. Baretto *et al.* (Baretto et al., 2002) and K. Harrison *et al.* (Harrison et al., 2002). For characteristic two the main result is the work *et al.*(Scott et al., 2006). The cost of their respective formulas are given in Table 1.

Table 1: Complexity comparison.

Method	Trip.	Mixed add.	Doub.
(Scott et al., 2006)	–	$9M+3S$	$1M+7S$
Proposed	–	$9M+5S$	$8S$
(Koblitz, 1998)	$6C$	$10M+1C$	
(Baretto et al., 2002)	$6C$	$9M+1C$	
(Harrison et al., 2002)	$M+6C$	$8M+3C$	$7M+2C$
Proposed	$8C$	$7M+3C$	$6M+4C$

In this paper we first propose a new coordinate system in characteristic 2 called the XZ-projective coordinate system. We provide in this system formulas for doubling and mixed addition. We propose also a new coordinate system for characteristic 3 called ML-projective coordinate system. Again we give formulas for adding, doubling and tripling. The cost of these formulas are given in Table 1

Table 1 shows that our formulas provide some improvement in the efficiency of curve operations.

This paper is organized as follows. Basic concepts and previous work on arithmetic on supersingular elliptic curves are summarized in Section 2. We present our contribution for supersingular curve in characteristic 2 (resp. 3) in Section 3 (resp. Section 4). Finally we briefly conclude in Section 5.

Ho Kim K. and Negre C. (2008).
POINT MULTIPLICATION ON SUPERSINGULAR ELLIPTIC CURVES DEFINED OVER FIELDS OF CHARACTERISTIC 2 AND 3.
In *Proceedings of the International Conference on Security and Cryptography*, pages 373-376
DOI: 10.5220/0001926103730376

Table 2: Curve operations Affine coordinates.

	Characteric2	Characteric3
Add	$\lambda = \frac{y_1+y_2}{x_1+x_2}$, $x_3 = \lambda^2 + (x_1+x_2)$, $y_3 = y_1 + 1$ $+\lambda(x_1+x_3)$,	$\lambda = \frac{y_1-y_2}{x_1-x_2}$, $x_3 = \lambda^2 - (x_1+x_2)$, $y_3 = (y_1+y_2) - \lambda^3$,
Doub.	$x_3 = x_1^4 + 1$, $y_3 = y_1^4 + x_1^4$	$\lambda = \frac{1}{y_1}$ $x_3 = x_1 + \lambda$, $y_3 = -(y_1 + \lambda^3)$,
Trip.	$-$	$x_3 = x_1^9 - b$, $y_3 = -y_1^9$.

2 ARITHMETIC ON SUPERSINGULAR ELLIPTIC CURVES

Given a finite group with underlying difficult discrete logarithm problem (DLP) and efficient group law, one could use this group to implement cryptographic protocols such as ElGamal encryption or Diffie-Hellman key exchange.

Recall that given a finite field $\mathbb{F}_{p^n}$ with p prime an elliptic curve E over $\mathbb{F}_{p^n}$ is the set of pairs $(x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ satisfying a Weierstrass equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where a_i for $i = 1,\ldots,6$ are constants in $\mathbb{F}_{p^n}$. Elliptic curves have a natural group structure given by chord and tangent method. This provides efficient group arithmetic and difficult DLP suitable for cryptographic applications.

In this paper we consider special elliptic curves, the supersingular elliptic curves defined over field of characteristic 2 and 3. Their equation are the following

$$E(\mathbb{F}_{2^n}) \quad Y^2 + Y = X^3 + X + b \text{ where } b \in \{0,1\} \quad (1)$$
$$E(\mathbb{F}_{3^n}) \quad Y^2 = X^3 - X + b \text{ where } b \in \{-1,1\} \quad (2)$$

These curves are really interesting for efficient implementation of pairing-based cryptosystems. Indeed, to implement protocol based on pairing on an elliptic curve $E(\mathbb{F}_q)$, the curve must have an embedded degree k not too big. The embedded degree is the smallest integer k such that the Tate pairing, for instance, can be computed. It has been shown that supersingular elliptic curves satisfy this condition (Galbraith, 2001).

In affine coordinates, operations on the curve can be computed using the following formulas give in Table 2

Since the proposition of ECC by Koblitz and Miller, research have been done to improve the cost of operations on the curve. We see in Table 2 that doubling and tripling is free of field inversion and field multiplication. But the other operations require inversion in affine coordinate.

A popular idea to avoid inversion in curve operations consists to use projective coordinates. The most interesting projective systems are the following

1. Ordinary projective $(X,Y,Z) \leftrightarrow (x,y) = (X/Z,Y/Z)$ in affine.
2. Lopez-Dahab projective $(X,Y,Z) \leftrightarrow (x,y) = (X/Z,Y/Z^2)$ in affine.
3. Jacobian projective $(X,Y,Z) \leftrightarrow (X/Z^2,Y/Z^3)$

Each system provides different operation cost for addition, doubling and tripling, but all of them avoid field inversion. Mixed addition is simply an addition with a point in the current projective system say P_1 and a second point P_2 in affine coordinate. It is generally cheaper than a general addition.

Field operations. Let us denote I a field inversion, M a multiplication, S a squaring and C a cubing in the ground field. These operations have different time consuming depending on the characteristic of the field. Specifically

- In characteristic two we have $I \gg M \gg S$ and $C = M + S$.
- In the case of characteristic three we have $I \gg M \cong S \gg C$ (see (Ahmadi et al., 2007)).

The curve operations are optimized regarding these relative costs of field operations.

3 OPERATIONS IN CHARACTERISTIC 2

In this section we present our work concerning arithmetic on an supersingular elliptic curve in characteristic 2. Specifically we would like to improve the arithmetic on the curve

$$E(\mathbb{F}_{2^n}) \quad Y^2 + Y = X^3 + X + b \text{ where } b \in \{0,1\}.$$

To reach this goal we use a new system of representation called XZ-projective coordinates. This system can be seen as an improvement of the Lopez-Dahab (Lopez and Dahab, 1998) projective coordinates.

Definition 1 (XZ-projective coordinates)**.** *The XZ-projective coordinates of a point P on an elliptic curve E is a quadruple (X,Y,Z,T) such that $T = XZ$ and the affine coordinate (x,y) of P are given by*

$$x = X/Z, \; y = Y/Z^2.$$

In this system we obtain the formulas given in the following proposition for addition and doubling on the curve defined by (1).

Proposition 1 (Curve operation in XZ-projective coordinate)**.** *Let $E(\mathbb{F}_{2^n})$ a supersingular curve defined by the following equation*

$$Y^2 + Y = X^3 + X + b \text{ where } b \in \{0,1\}.$$

Let $P_1 = (X_1, Y_1, Z_1, T_1)$ and $P_2 = (X_2, Y_2, 1, T_2 = X_2)$ be two points on $E(\mathbb{F}_{2^n})$ expressed in XZ-projective coordinates. Then

Mixed Addition. *Let $P_3 = P_1 + P_2$, the XZ-coordinates (X_3, Y_3, Z_3, T_3) of P_3 can be computed as*

$$\begin{aligned} Z_3 &= (X_2Z_1^2 + T_1)^2, \quad T_3 = X_3Z_3, \\ X_3 &= (X_2Z_1^2 + T_1)(X_2Z_1 + X_1)^2 \\ &\quad + (Y_2Z_1^2 + Y_1)^2, \\ Y_3 &= Z_3^2(Y_2 + 1) \\ &\quad + (X_2Z_3 + X_3)(X_2Z_1^2 + T_1)(Y_2Z_1^2 + Y_1). \end{aligned} \tag{3}$$

And the cost of these formulas is $9M + 3S$

Doubling. *Let $P_3 = 2P_1$, the XZ-coordinates (X_3, Y_3, Z_3, T_3) of P_3 can be computed as*

$$\begin{array}{lllllll} X_3 & = & (X_1 + Z_1)^4, & Y_3 & = & (Y_1 + T_1)^4, \\ Z_3 & = & (Z_1^2)^2, & T_3 & = & (T_1 + Z_1^2)^4. \end{array} \tag{4}$$

The cost of these formulas is equal to $8S$.

Proof. Mixed Addition. To prove that the formulas (3) are correct, we have to prove that X_3/Z_3 and Y_3/Z_3^2 are equal to the expression of x_3 and y_3 in Table 2. Using (3) we have

$$X_3/Z_3 = \frac{(X_2Z_1^2 + T_1)(X_2Z_1 + X_1)^2 + (Y_2Z_1^2 + Y_1)^2}{(X_2Z_1^2 + T_1)^2}.$$

If we factorize Z_1^4 in the numerator and the denominator we get

$$\begin{aligned} X_3/Z_3 &= \frac{(X_2+X_1/Z_1)(X_2+X_1/Z_1)^2+(Y_2+Y_1/Z_1^2)^2}{(X_2+X_1/Z_1)^2} \\ &= (x_2 + x_1) + \left(\frac{y_2+y_1}{x_2+x_1}\right)^2. \end{aligned}$$

This means that X_3/Z_3 satisfies equation of Table 2. Now let do the same thing in the expression of Y_3/Z_3^2

$$\begin{aligned} Y_3/Z_3^2 &= (Y_2 + 1) + \frac{(X_2+X_3/Z_3)(X_2Z_1^2+T_1)(Y_2Z_1^2+Y_1)}{Z_3} \\ &= (Y_2 + 1) + \frac{(X_2+X_3/Z_3)(X_2+X_1/Z_1)(Y_2+Y_1/Z_1^2)}{(X_2+X_1/Z_1)^2} \end{aligned}$$

but this last expression is equal the expression of Table 2.

Doubling. This case is simpler, and the proof is similar to the proof of addition formulas. For the sake of simplicity we leave this part to the reader.

□

Now let us compare our formulas with best known formulas for curve $E(\mathbb{F}_{2^n}$ defined by

$$Y^2 + Y = X^3 + X + b \text{ where } b \in \{0,1\}.$$

We reported the cost of these formulas (Scott et al., 2006) reported in Table 3.

Table 3: Complexity comparison.

Algorithm	Coord.	Doubling	Mixed add
Classic	Aff.	$4S$	$I + 2M + S$
(Scott et al., 2006)	Jac.	$M + 7S$	$9M + 3S$
Proposed	XZ-proj.	$8S$	$9M + 5S$

We can see that the doubling is cheaper by $1M$ compared to Scott. In counter part,we have one more squaring int the doubling, and two more squaring in the addition.

4 OPERATIONS IN CHARACTERISTIC 3

We propose a novel system of representation called ML-projective coordinates. This system can be seen as an improvement of the original Jacobian coordinate.

Definition 2. *The ML-projective coordinate of a point P on an elliptic curve E is quadruplet (X, Y, Z, T) such that $T = Z^2$ and the affine coordinate (x,y) of P are given by*

$$x = X/T, y = Y/Z^3.$$

In this system we found different formulas for point addition, point doubling and point tripling on an elliptic curve defined by (2).

Proposition 2 (Curve operation in ML-projective coordinate)**.** *Let $E(\mathbb{F}_{3^n})$ a supersingular curve defined by the following equation*

$$E(\mathbb{F}_{3^n}) \; Y^2 = X^3 - X + b \text{ where } b = \pm 1$$

Let $P_1 = (X_1, Y_1, Z_1, T_1)$ and $P_2 = (X_2, Y_2, 1, 1)$ be two points on $E(\mathbb{F}_{3^n})$ expressed in ML-projective coordinates. Then

Addition. *Let $P_3 = P_1 + P_2$, the ML-coordinates (X_3, Y_3, Z_3, T_3) of P_3 can be computed as*

$$\begin{aligned} Z_3 &= Z_1(X_2T_1 - X_1), \; T_3 = Z_3^2, \\ X_3 &= (Y_2Z_1^3 - Y_1)^2 + (X_2T_1 - X_1)^3 \\ &\quad + X_2T_3, \\ Y_3 &= (Y_2Z_1^3 + Y_1)(X_2T_1 - X_1)^3 \\ &\quad - (Y_2Z_1^3 - Y_1)^3. \end{aligned} \tag{5}$$

These formulas require $7M + 3C$.

Table 4: Complexity comparison.

Algorithm	Coordinates	Tripling	Mixed addition	Doubling
Classic	Affine	$4C$	$1I+2M+1C$	$1I+1M+1C$
(Koblitz, 1998)	Ordinary projective	$6C$	$10M+1C$	-
(Baretto et al., 2002)	Ordinary projective	$6C$	$9M+1C$	-
(Harrison et al., 2002)	Jacobian	$1M+6C$	$8M+3C$	$7M+2C$
Proposed	ML-Projective	$8C$	$7M+3C$	$6M+4C$

Doubling. *Let $P_3 = 2P_1$ the ML-coordinates (X_3, Y_3, Z_3, T_3) of P_3 can be computed as*

$$\begin{array}{rcl} Z_3 & = & -Y_1Z_1^3, \;\; T_3 = Z_3^2, \\ X_3 & = & (T_1^3)^2 + (X_1^3 - Y_1^2)Y_1^2 + bT_3, \\ Y_3 & = & T_1^9 + Y_1^2T_3. \end{array} \qquad (6)$$

These formulas require $6M+4C$.

Tripling. *Let $P_3 = 3P_1$ the ML-coordinates (X_3, Y_3, Z_3, T_3) of P_3 can be computed as*

$$\begin{array}{rclrcl} X_3 & = & (X_1 - bT_1)^9, & Y_3 & = & -Y_1^9, \\ Z_3 & = & Z_1^9, & T_3 & = & T_1^9. \end{array} \qquad (7)$$

These formulas require $8C$.

Proof. Mixed Addition. Let us check that X_3/T_3 and Y_3/Z_3^3 are equal respectively to x_3 and y_3 of Table 2. For X_3/T_3 we have

$$\begin{array}{rcl} X_3/T_3 & = & \frac{(Y_2Z_1^3-Y_1)^2+(X_2T_1-X_1)^3+X_2T_3}{T_3} \\ & = & \frac{(Y_2Z_1^3-Y_1)^2+(X_2Z_1^2-X_1)^3}{\left(Z_1(X_2Z_1^2-X_1)\right)^2} + X_2 \end{array}$$

since $T_1 = Z_1^2$. We proceed the simplifications

$$\begin{array}{rcl} X_3/T_3 & = & \frac{(Y_2Z_1^3-Y_1)^2}{Z_1^2(X_2Z_1^2-X_1)^2} + \frac{X_2Z_1^2-X_1}{Z_1^2} + X_2 \\ & = & \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - (x_2+x_1). \end{array}$$

After the cancellation of the power of Z_1 in the numerators and denominators we get the required expression (Table 2).

For Y_3/Z_3^3 and for Doubling and Tripling formulas we can prove it in the same way.

□

In Table 4 we give the cost of the operation in ML-coordinate and also the cost of the best known formulas ((Koblitz, 1998; Baretto et al., 2002; Harrison et al., 2002)). We remark that our formulas improve previous mixed addition formulas by $1M$ or $2M$. In on other hand, the tripling require 2 more cubing.

5 CONCLUSIONS

In this paper we have studied the arithmetic on supersingular elliptic curve defined over field of characteristic 2 and 3. We have introduced two new coordinate systems , the XZ-projective coordinates and the ML-projective coordinates. We obtain new formulas for point addition, point doubling and point tripling on the curve. The formulas are cheaper and provide a more efficient scalar multiplication on the curve.

REFERENCES

Ahmadi, O., Hankerson, D., , and Menezes, A. (2007). Software implementation of arithmetic in GF(3^n). In *WAIFI 2007*.

Baretto, P. S. L. M., Kim, H. Y., Lynn, B., and Scott, M. (2002). Efficient algorithms for pairing based cryptosystems. In *CRYPTO'2002*, volume 2442, pages 354–368.

Galbraith, S. D. (2001). Supersingular curves in cryptography. *Lecture Notes in Computer Science*, 2248.

Hankerson, D., Menezes, A., and Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer-Verlag.

Harrison, K., Page, D., and Smart, N. P. (2002). Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems. *LMS J. Comput. Math.*, 5:181–193.

Koblitz, N. (1998). An elliptic curve implementation of the finite field digital signature algorithm. In *CRYPTO'98*, volume 1462, pages 327–337.

Lopez, J. and Dahab, R. (1998). Improved algorithms for elliptic curve arithmetic in GF(2^n). In *SAC'98*, pages 201–212.

Page, D. and Smart, N. P. (2002). Hardware implementation of finite fields of characteristic three. In *4th CHES'2002*, volume 2523 of *LNCS*, pages 529–539. Springer.

Scott, M., Costigan, N., and Abdulwahab, W. (2006). Implementing cryptographic pairings on smartcards. In *CHES 2006*, volume 4249, pages 134–147.